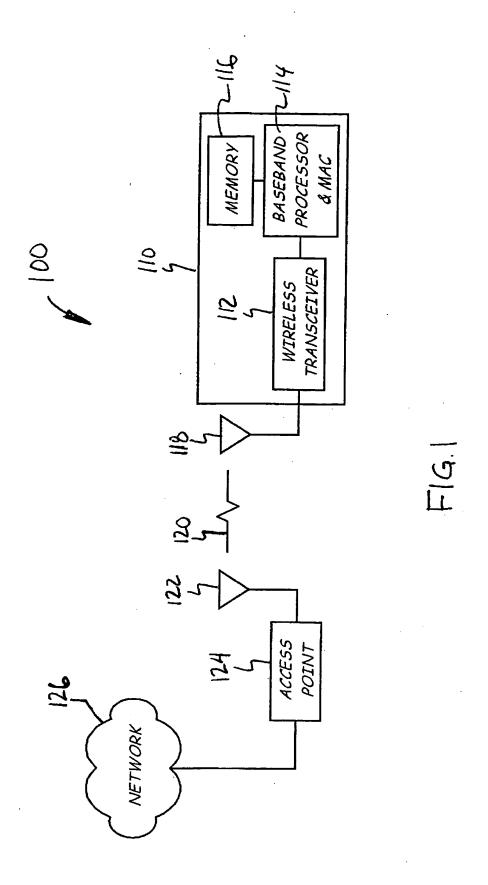
"Authenticated Key Exchange Based On Pairwise Master Key"
by Jesse Walker
Docket #: P15875
Contact: Kenneth J. Cool @ (719) 273-1090, Reg. No.: 40,570
Sheet 1 of 3



"Authenticated Key Exchange Based On Pairwise Master Key" by Jesse Walker

Docket #: P15875
Contact: Kenneth J. Cool @ (719) 273-1090, Reg. No.: 40,570
Sheet 2 of 3

| COMMUNICATION | INFORMATION TRANSFERRED | | |
|---|-------------------------|--|--|
| $AP \rightarrow STA$ (PROBE RESPONSE) | ANONCE | | |
| STA → AP (REASSOCIATE REQUEST) | ANONCE, SNONCE, MICI | | |
| $AP \rightarrow STA$ (REASSOCIATE RESPONSE) | SNONCE, MIC2 | | |

| | | FI <i>G</i> . 2 | | |
|---------------|----------------|--------------------|--|--|
| | | 300 | | |
| Element ID | Length 1 octet | Nonce 32 octets | | |
| | | | | |

F14.3

| | | - | | , | ,400 |
|--------------------------|----------------|--------------------|---------------------|---------------------|------------------|
| Element ID I octet | Length 1 octet | Key ID 8 octets | ANonce 32 Octets | SNonce 32 Octets | MIC 16 octets |
| I octet | | | 32 Octets | | |

F16 4

| 1 octet 8 octets Length GTK length 6 October 1990 | | | , | | | (| 200 |
|--|----|-------------|----------|------------|-----------------|---------------------|------------------|
| 1 octet 1 octet 1 octets 32 octets 16 octets | ID | | Length | GTK length | RSC 6 Octets | GNonce 32 Octets | MIC 16 octets |

F16. 5

Docket #: P15875
Contact: Kenneth J. Cool @ (719) 273-1090, Reg. No.: 40,570
Sheet 3 of 3

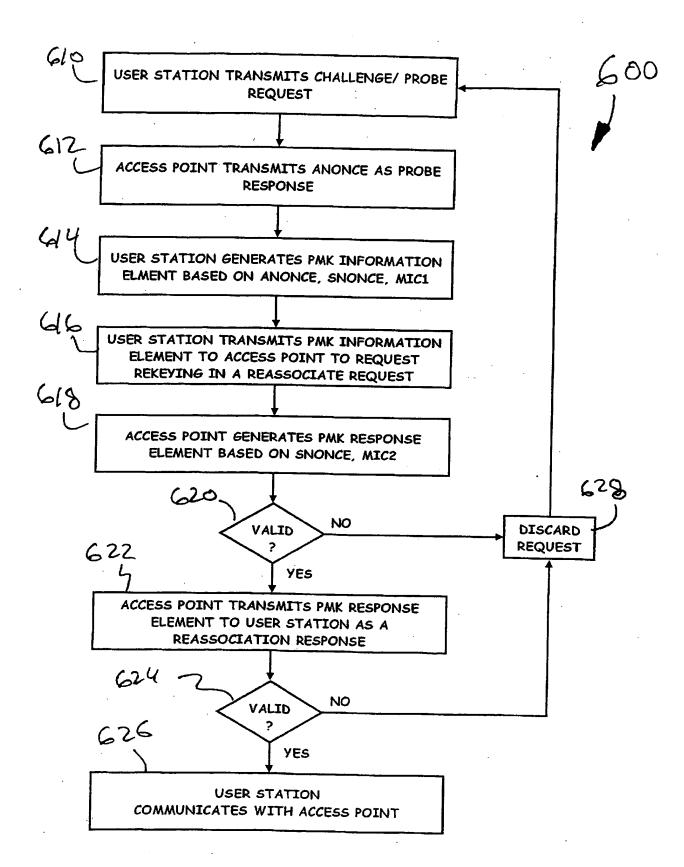


FIG. 6